LA-UR-21-23847
Approved for public release; distribution is unlimited.

Title: System Administrator Training Item #25928

Author(s): Rinke, Helen Mae

Intended for: Training

Issued: 2021-04-20

System Administrator Training
Item #25928

Introduction

External and internal cyber-attacks pose an extreme risk to government, businesses and individuals. System attacks, resulting in compromised information are occurring more frequently and the threat to the Laboratory has never been higher.

This training has been developed to help you better understand your role as a System Administrator and recognize your responsibilities within the Laboratory's Information Security (Cyber) Program and has been revised to address newly implemented ACD 470.6 restrictions for mobile devices in secure areas.

LANL considers a system administrator/privileged user as someone who has unrestricted access rights to more than one computer which contains other people's information and data on assets within an information system. This training primarily addresses the System Administrator, however it is applicable to all privileged users such as; network and database administrators, IT developers, webpage designers, security and audit personnel.

Threats to the security and stability of LANL's information systems are constantly evolving, so every computer user--especially users with elevated privileges--must diligently manage and protect their system and electronic information. Never underestimate the importance of each person in securing our information and serving LANL's mission.

Each month LANL records millions of unauthorized attempts to gain access to its computing systems. So far, our track record in preventing loss of information and damage to computing systems has been excellent. But we cannot let down our guard. The methods being used to gain unauthorized access to computing systems are constantly changing. Each computer user is an important link in the LANL information security chain.

You can adjust the **font size** using the controls on the lower left side of the page. You can also use the **1** through **5** keys on your keyboard, where **1** is **extra small** and **5** is **extra large**. Your font size preference will be remembered for up to a year, less if you delete your web browser's cookies.

This course (#25928) has been DC reviewed and has been deemed unclassified xxxxxx

LANL's Information Security Program

The LANL Information Security Program protects LANL hardware, software, and communication systems from both external and internal attacks. The program identifies and implements procedures to secure the confidentiality, integrity and availability of LANL information systems. It is the Laboratory's goal to manage all aspects of the information security program in a manner that achieves mission deliverables, protects the information entrusted to it, and complies with contractual information security requirements.

The information security program policies and procedures cover many areas. These include:

- Certification and Accreditation via CIO-P310 CIO Procedure for POA&Ms and CSIP
- Audits, Self-Assessments and Verification and Validation via CIO-P230 Cyber Audits and Accountability
- Contingency Planning and Disaster Recovery tied to CIO-P310 CIO Procedure for POA&Ms and CSIP
- Secure Administration and Configuration Management via CIO-P250 Information Technology Configuration Management
- Access Control via P218 Cyber Security Controls and CIO-P350 Oracle Responsibilities-Assignment, Review and Revocation
- Least Privilege and Need to Know via P218 Cyber Security Controls
- System Monitoring via CIO-P230 Cyber Audits and Accountability and CIO-P240 System and Information Integrity
- Incident Management via P214 Cyber Information Security Incident Management
- Sanitization via PD210 Cyber Security Program and P211 Transfer and Sanitizing of Electronic Storage Media
- Controlled Portable Electronic Devices via P217 Controlled Portable Electronic Devices
- Wireless Devices via P213 Cyber Security Wireless Computing Devices
- Training and Awareness via P220 Information Security Education and Awareness

Course Objectives

At the conclusion of this course you will be able to:

- Describe the LANL Information Security Program
- Recognize Information Security Roles
- Recognize required Information Security training requirements
- Describe the role of the System Administrator
- State your responsibilities and authority as a System Administrator
- Describe Incident Management and the Role of the Security Incident Team [SIT]
- Report Information Security incidents
- Describe Information Spillage and the Contamination Cleanup
- Explain access control principles, such as need to know, and least privilege
- Implement LANL User Access Controls
- Support Audits, Self-Assessments, and Verification and Validation
- Describe your responsibilities for wireless controls
- Describe Contingency Planning for information systems
- Explain Certification and Accreditation of information systems
- Identify the CIO policy for Internet-Accessible Services and the training required for system administrators

. LANL Information Security Roles

Many roles are involved in managing information security at the Laboratory. These include:

- Authorizing Official (Los Alamos Field Office)
- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Information System Security Manager (ISSM)
- Information System Owner (ISO)
- Responsible Line Manager (RLM)
- Information System Security Officer (ISSO)
- Organizational Cyber Security Representative (OCSR)
- Senior Cyber Security Advisor (SCSA)
- Cybersecurity Technical Staff (CTS)
- Contingency Plan/Disaster Recovery Coordinator (CP/DR)
- Classified and Unclassified System Administrators

The Laboratory trains and entrusts all levels of management and workers to accept responsibility for portions of the Information Security Program under their control, and will hold all Laboratory workers accountable for their actions in relation to those responsibilities.

Anyone serving in information security roles must follow procedures to protect the hardware, software, and network (communications) infrastructure from attacks or leaks of information that would compromise the Confidentiality, Integrity and Availability (CIA) of information.

See PD210, Cyber Security Program.

System Administrator Training

System Administrator training is an integral part of information security. Keep all of your unclassified and classified training up to date. This course that you are currently taking is in the institutional training plan 4971 SYSTEM ADMINISTRATOR ACCESS.

Training plan 7870 SECURE INTERNET ACCESSIBLE-SERVICES and course 34428 Secure Web Applications Awareness are required for owners, RLMs, developers and System Administrators for web servers on the Green Network. See the Internet-Accessible Services section of this training.

The System Administrator role is critical to keeping IT at the laboratory running and free of vulnerabilities. Work with your RLM and ISSO to chart a progressive training program or certifications for the systems you support to improve your technical skills.

The Role of System Administrator

System Administrators can have unrestricted access to a computer operating system, software and data. System Administrators can also have unrestricted privileged access to organizational servers, information system computers, operating system, software and data.

System administrators are privileged users who are support personnel who manage computer equipment (e.g., networks, servers, and workstations) for a Laboratory organization by performing a wide range of professional functions such as:

- Configuring the system
- Supporting, and maintaining servers
- Developing scripts or programs to perform management functions
- Troubleshooting operational issues
- Installing software and hardware
- Allocating system resources to users
- Creating and deleting user accounts
- Granting other users appropriate authorities consistent with their access rights

The number of System Administrators with access to computer equipment is limited to the minimum number needed to manage the system.

To make sure there is a separation of duties "A single employee may not be appointed to perform both roles of System Administrator and ISSO for a classified system as referenced in section 4.8 of PD210 Cyber Security Program."

System Administrator Responsibilities

Privileged users and system administrators must:

- Be United States citizens, unless otherwise approved in accordance with the approved Information System Security Plan (ISSP) or in writing by the Authorizing Official. Non US citizens are explicitly prohibited from being privileged users on classified systems.
- Comply with all requirements applicable to general users.
- Ensure that user access to the information system (at the desktop or network level) is based on the least privilege principle.
- Ensure that user access to the information system (at the desktop or network level) is based on a need to know.
- Possess an access authorization sufficient for access to the highest classification and most restrictive category of data processed on the information system.
- Use unique identifiers as described in the approved information system security plan.
- Protect the administrator, root or super-user authenticator at the highest level of data it secures.
- Be responsible for all super-user or root actions under their accounts.
- Use the special access or privileges granted only to perform authorized tasks and functions.
- Opt for the least privilege while computing. Use your general user account for all actions that do not require elevating to a privileged user account. Pay particular attention to the access of web sites. Browsing with administrative access is extremely dangerous and can compromise the system.
- Work closely with the ISSO to coordinate activities, such as identifying system vulnerabilities, adding of hardware and software, and system maintenance.

System Administrator Authority

System Administrators must:

- Stop system operations if there is an unsafe or unsecure situation.
- Report security and safety concerns to management.
- Protect access to passwords and CRYPTOCard Personal Identification Numbers (PINs) from other personnel.
- Implement the security controls specified in the ISSP.
- Deny access to the system based on the procedures for the system.
- Access all system resources to fulfill the duties of the privileged user.
- Ensure that cyber security incidents are reported in compliance with *P214, Information Security Incident Management.*

The Security Incident Team

The SIT (Security Incident Team) provides a central point of contact for reporting security incidents, including information security incidents. The goal of each inquiry is to determine if a security compromise occurred and whether national security was at risk or damaged. Every inquiry also identifies causal factors to make improvements.

Incident Management gives the Laboratory a way to handle Information Technology problems, or incidents, in a consistent way by using the same process, the same tool, and the same information to resolve and ultimately improve processes and procedures.

Incidents of security concern are actions, inactions, or events that:

- Pose threats to national security interests and/or critical DOE assets.
- Create potentially serious or dangerous security situations.
- Potentially endanger the health and safety of the workforce or public.
- Degrade the effectiveness of the Security and Safeguards (S&S) program.
- Adversely impact the ability of organizations to protect DOEs interests.
- Include suspected potential unauthorized disclosures of PII, classified or CUI.

The SIT conducts inquiries to ascertain facts surrounding each incident and manages the reporting processes for the incidents.

Anyone who witnesses or has knowledge of activities, omissions, or acts that potentially represent a violation of information security requirements, or circumvention, intended or not, of information security controls is ***required*** to report the incident to the SIT.

Reporting occurrences ensures that Laboratory management and federal oversight are fully informed of all events that might adversely impact security interests; helps establish a system for determining and taking the appropriate corrective action.

Reporting an Incident

Report incidents promptly to the SIT by phone at 665-3505 to your DSO, and RLM. Use caution when reporting an incident involving classified information through insecure means.

Recommendations:

- Be careful when reporting a possible classified incident; if possible speak to the SIT or your DSO in person.
- To reduce the impact of an incident and ensure prompt external reporting, known or suspected incidents should be reported immediately after their discovery.
- Self-reporting incidents is encouraged.
- Report incidents first to the Security Incident Team (SIT) or your Deployed Security Officer (DSO), then to the RLM, SCSA or Deployed Security Officer (DSO), and the OCSR.
- Report the disclosure of classified information in person.
- Never discuss classified details over an unsecure phone line.
- Don't provide classified details in an unclassified email.

Information Spillage/Contamination Cleanup

Spillage is the release of information of lower level systems with material a higher category of information than the system is accredited to contain. This is referred to as a contamination. LANL personnel with a potential or verified contamination, including sub-contractors, must report and follow instructions given by the SIT. The SIT and LANL's Office of Classification will make a determination if there has been a contamination and the classification of the information. Once a contamination has been verified there will be a formal inquiry to determine the scope of the contamination.

When a possible contamination may have occurred the person who identified it must report it to the SIT by phone at (505-665-3505), or by email at sit@lanl.gov as soon as possible. **Use caution when reporting an incident involving classified information through insecure means.**

The SIT coordinates with System Administrators, computer technicians, and others in the process of contamination cleanup (sanitization), which is the clearing, purging, or destruction of computer media in order to remove malicious, classified or sensitive data from computers. See

CIO-P290, *Information Spillage Cleanup Policy* for specific information about identifying, reporting, verification and cleanup of contaminations.

Access Control Principles

The importance of protecting computer systems and networks cannot be underestimated. Protection measures should be followed to protect against external and internal threats.

The access principles used for systems at the Laboratory are:

- **Need to Know**
  Need to know is an access determination that ensures a worker is only accessing data that they need to know to do their job, and that access to that data is based on necessity in performance of the worker's official or contractual tasks, duties, and assignments.
- **Least Privilege**
  The principle of 'least privilege' means giving a user only those access privileges that are essential for the user's work. For example, users could be given read/write access on files within their own directory, but would not be permitted to modify other files on a server. ***Privileged users must not access their email or the internet using a privileged account unless the client is configured to not automatically run mobile code, such as ActiveX, Flash, PDF and Java.***
- **Separation of Duties**
  The 'separation of duties' principle applies both to systems and operators, and/or users. Separation of duties helps ensure that, as appropriate, multiple people are involved in the protection of the system and information. The RLM ensures that checks and balances exist for privileged access by enforcing a separation of duties.
- **RLM Access Determination and Approval**
  To help assure the principle of 'least privilege' is followed, the RLM approves the level of system access for each user based on the appropriate, minimum needs of tasks, functions, or processes required for the user to perform their job. The RLM for the information system approves user access to an information system. The RLM must ensure that all access is approved based on the individual's clearance level, 'need-to-know,' 'least privilege,' and 'separation of duties' principles, where appropriate and is renewed annually by the RLM.

LANL User Access Controls

System Administrators must implement access controls required for all LANL computer users. These controls are listed in P218 Cyber Security Access Controls. In particular, System Administrators should become expressly familiar with the following Password/PIN requirements from P218:

- Multi-factor authentication methods using:
  - Using PIV Cards
  - Passcodes – Unclassified and Classified
  - A CRYPTOcard- Unclassified and Classified
- Passcode/Personal Identification Number (PIN) Requirements-Unclassified
- Passcode/Personal Identification Number (PIN) Requirements-Classified
- Control of Legacy Authentication Methods

All systems must provide the following for authentication and access control:

- A unique association between a user's account name (identification) and password (authentication).
- Account authorization(s) and account privilege(s).

The identification and authentication processes of each system must ensure that a user can only access authorized cyber assets and information. These processes must be managed with a degree of rigor appropriate to the classification level of the information system. The System Administrator must follow all access control requirements, particularly the following:

- All local privileged accounts must be denied direct access from the network.
- Passwords to shared, privileged, and local accounts must be changed anytime anyone who knows the password transfers, leaves, or is reassigned.
- Any account that must be shared with a known static or multi-use password cannot be directly be accessed across the network; such accounts can be accessed only at the system console.
- The same password may **not** be used on multiple systems or applications. This is especially important for System Administrator accounts on multiple computers or systems.
- All lapses of password security must be reported to the SIT as soon after discovery as possible.
- Access approvals to unclassified systems are managed both through the access authorization process of the local system and the network.
- Any deviations from the unclassified authentication requirements must be registered with, and approved by, the Laboratory Chief Information Security Officer (CISO).
- User passwords used for processes running on the system on behalf of a user or stored within a script must be changed anytime the user transfers, leaves, or is reassigned, when technically feasible.
- All factory- and vendor-configured privileged accounts are disabled (i.e., the account password will be set to a random string).
- All access to LANL Yellow Network computing resources by uncleared foreign nationals must be controlled through the Open Collaboration Enclave (OCE).

Access Control Quick Tips

Here are some quick tips for access security controls:

- Computer passwords and PINS must be protected at the highest classification level of the information on the system.
- Robust credentials must be used for authentication. The requirements for configuration and management of credentials are available in the posted Job Aids: https://int.lanl.gov/org/ddops/aldbus/cio/job-aid.shtml.
- It is the responsibility of the worker's RLM or other approving official to ensure that access to information systems is based on the user's security clearance and 'need-to-know' to perform the assigned job, where appropriate.
- Never share passwords or pins with ***anyone***.
- Inform your RLM if you are asked for your password or PIN.
- All assets left unattended will be physically protected from unauthorized access (e.g. in a locked office), logged off, or protected using a screen lock.
- Screen locks should be set to 15 minutes of inactivity and password protected.

Audits, Self-Assessments, and Verification and Validation

As a System Administrator, you may be asked to prepare information for Audits, Self-Assessments/ Verification and Validation (V&V). The goal of these programs is to:

- Ensure that protection measures are implemented and functioning as documented.
- Help discover security concerns and weaknesses.
- Assist in resolving issues in order to lower the risk to the Confidentiality, Integrity and Availability (CIA) of information.

Verification and Validation (V&V) is a process used to safeguard information security. Verification means determining that a Laboratory system meets a specific set of designated security specifications, regulations or requirements, and can identify opportunities for improvement. Validation is an analysis intended to ensure that each computer system meets the user's operational needs. For example, a V&V was conducted to verify that PII did not exist on an organization's computers.

If you are asked to work with auditors, here are some tips to keep in mind.

- Be courteous. Answer questions honestly and to the best of your ability.
- LANL employees are required to provide information requested within the scope of the audit, please provide it to the Office of the Chief Information Officer (OCIO). OCIO will record it and distribute to the auditors.
- Respond to auditors as quickly as possible.
- Only answer the question that is being asked.

- If you don’t know the answer to a question, say so. There is no need to speculate with your answers. Let the auditor know you don’t know but will find out and provide the information to OCIO.
- Be as clear and brief in your answers as possible while answering the question.
- Be aware of the auditor’s security clearance level. They may not be authorized to know the information they are asking about. It may also be outside the scope of their audit. Be careful in promising them classified information.
- Don’t argue with an auditor.
- During an audit interview the employee has the right to have their supervisor, the system ISO and/or ISSO, an OCIO representative or other LANL personnel, present during the interview. This is a recommended practice

Wireless Controls

Wireless controls in P213 Cyber Security Wireless Computing Devices applies to Laboratory workers and visitors who have access to or manage access to LANL information systems. The procedure provides the framework to manage and use wireless-enabled devices at the Laboratory. P213 can help you to do the following:

- Identify what types of wireless activities are allowed.
- Know the requirements and responsibilities for the use of wireless devices.
- Implement the requirements on LANL systems.

A LANL Wireless System Security Plan must be approved the Authorizing Official for the following:

- Information systems using wireless networking.
- Systems in Limited Areas that require a cell phone connection to a LANL network.
- Bluetooth communications between computing devices and peripherals.
- Nonstandard wireless computing devices.

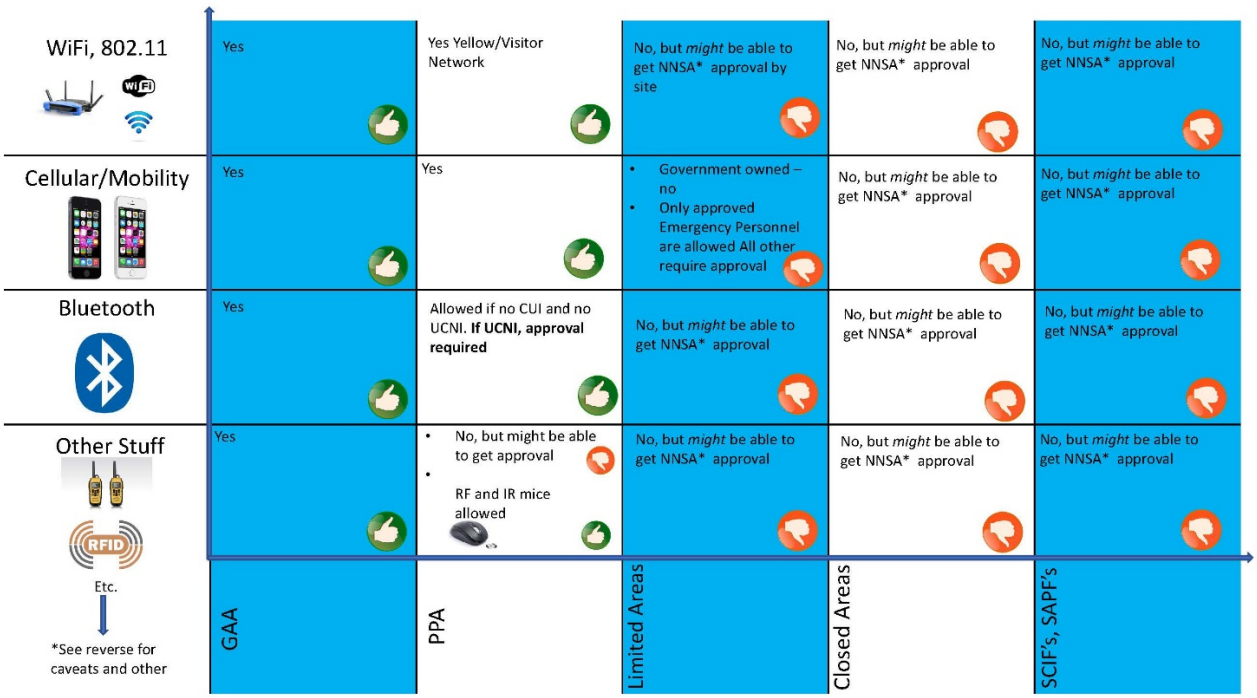
Wireless is not allowed on classified systems. A security plan for wireless controls is required. All controls must be tested. A plan must be proposed for the following types of wireless systems:

- Information systems using wireless networking on LANL property.
- Systems in limited Areas that require a cell phone connection to a LANL network.
- Bluetooth communications between computing devices and peripherals.

- Nonstandard wireless computing devices.

Wireless Controls cont.

Per 470.6 Use of Mobile Devices Within National Nuclear Security Administration Secure Spaces Advance Change Directive (ACD) it's important that you are able to recognize the requirements for using Wi-Fi, cellular, Bluetooth and other technology in Laboratory areas to report unauthorized use. The charts below can help.



Site Specific Rules

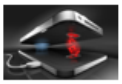
In addition to Laboratory-wide rules, there could be site-specific rules for wireless use that varies from building to building. The RLMs for the organizations set these requirements. System Administrators should consult with the RLMs to verify the requirements or if they have any questions.

Keyboards:

- RF (Wireless of any kind)
- Infrared (IR) – Can be used on unclassified systems in PPA's that do not process CUI.

Other IR:

- IR data communications are allowed between unclassified systems in PPA's that do not process CUI.



Remote controls:

- RF and IR remote controls on unclassified presentation equipment is allowed in unclassified work space.
- RF and IR remote controls not allowed on classified systems.

*Any RF (Wireless of any kind) requires a NNSA Headquarters approval of a TEMPEST Transmitter Review Form (TRF) for any RF within 100 feet of classified computing or if it will be introduced to a Limited Area or higher where classified computing takes place. **A strong business case is needed!**

** Wireless devices may also be considered Controlled Articles (such as smart phones). Please review *P217 Controlled Articles* and *P213 Cyber Security Wireless Computing Devices* prior to introducing such devices. For policy questions, you may also contact the Senior Cyber Security Leader list at scsl@lanl.gov

Responsibilities for Wireless Computing

System Administrators may be asked to configure or connect computers to wireless systems. Work with the system ISSO for the hardware/device requirements and rules of use. Possible tasks include:

- Configuring Entrust encryption
- Connecting Laptops to wireless internal networks
- Adding wireless peripherals
- Determining what hardware is wireless
- Disabling devices

Contingency Planning

Every accredited information system at the Laboratory is required to have an approved Contingency Plan.

Contingency Planning ensures the delivery of service or data during or after a crisis and for robust IT systems, reduced downtime and risk, and improved procedures. Contingency planning shows the interdependencies of IT systems, illustrates single-points-of-failure, delivers cost/benefit analysis for spare equipment, details data backup strategies, and offers all parties a roadmap when a crisis occurs. A Business Impact Analysis is also conducted as part of Contingency Planning. A Contingency Plan is required for all accredited systems. Annual Contingency Plan testing is required.

For information systems the Contingency Plan identifies:

- The system location
- Data sensitivity
- Contingency situations

- Assumptions
- Risks
- Vulnerabilities
- Major impacts
- Recovery procedures
- And more

The ISSO for the system and the Laboratory Contingency Planning Coordinator can provide specific information.

Additional Contingency Planning Responsibilities for System Administrators

System Administrators also need to do the following:

- Know user attributes, i.e. citizenship, clearance level.
- Be able to identify privileged users for RED and OCE access.
- Know what safeguards are in place.
- Know your location constraints.
- Assign user access.
- Know how your system works with CRYPTOcard authentication.
- Know how to trouble shoot problems.
- Monitor excessive login attempts and failures.

Certification and Accreditation

The Laboratory requires Certification and Accreditation of all Information System Security Plans. Certification and Accreditation categorizes systems based on risk and consequence of loss, and evaluates mitigating controls to ensure the security of the systems. The LANL Information Security Site Manager (ISSM) and Deputy ISSM using Certification Agents to certify the protection requirements of the ISSP are operational and residual risk, after mitigations, is acceptable for Approval to Operate by the appropriate Authorizing Official under the Risk Management Framework (RMF) model.

The LANL ISSM also develops the Cyber Security Program implementation for all information systems, ensuring that only NNSA-approved security configurations are implemented. The appropriate Authorizing Official certifies that the protection requirements described in the Information System Security Plan (ISSP) are operational in order to obtain Approval to Operate. Those that are often involved in the (process to obtain an Approval to operate include the ISSM, CISO, and ultimately the Authorizing Official.

The Certification and Accreditation process ensures that all security controls that are documented in the system's Information System Security Plan are implemented. This is achieved, in part through reviews, tests, and annual self-assessments.

Internet-Accessible Services

The Laboratory operates production and research services that are accessible to the public or to external users via the Internet. These web servers generally operate on the LANL internet facing "Green" network and are more exposed to intrusions than systems behind the LANL institutional unclassified "Yellow" network firewall. Compromised web sites serve as the entry points for intrusions within federal information systems.

Failure to implement a properly configured and managed web server introduces misconfigured servers, which allow for the disclosure or alteration of proprietary or sensitive information, including Publically Identifiable Information (PII). Networks can be exploited by attacks through the use of administrative credentials.

CIO-P270, Requirements for Internet-Accessible Services, specifies the requirements for web servers such as:

- Resilience
- Preventing software vulnerabilities
- Lifecycle planning and resourcing
- Vulnerability scans and continuous monitoring
- Requirements for system owners/operators

System Administrators for these web servers must be aware of the requirements. Training is required for owners, RLMs, developers and System Administrators for public facing web servers. As previously mentioned in System Administrator Training Section, training plan 7870

Secure Internet Accessible Services and course #34428 Secure Web Applications Awareness are required. See the System Administrator Training section for the training plan and course information.

Information Security Resources

Know your ISSO! The ISSO is your first point of contact if you have any questions. If your ISSO is not available, AskIT at 665-4444 can assist you during normal working hours.

For more information and to identify your ISSO see https://int.lanl.gov/org/ddops/aldbus/cio/ISSO.shtml.

https://int.lanl.gov/org/ddops/aldbus/cio/index.shtml has information about security controls. Individual links are provided for the following:

- CIO & Institutional Policies
- Information Architecture (IA) Standards
- Job Aids
- Certification & Accreditation

Reporting Incidents

To report Incidents of security concern contact the Security Incident Team (SIT) by phone at 665-3505, or by email at sit@lanl.gov. Information about the SIT can be found at https://int.lanl.gov/security/sit.shtml.

GETTING CREDIT FOR THIS COURSE

By requesting credit for this training, I acknowledge that I have read and understand the content of this training and that I will follow and meet requirements of this training, unless it is unsafe to do so.